Abstract

[0074] The invention relates to an authentication protocol for increasing safety against a man-in-the-middle (MITM) access attack for point-to-point communication (10), between client computer (12) and server (14), to services. The server (14) responds with an N byte nonce value and the client computer (12) utilizes a hash algorithm to compute a hash value of the parameters clients' password, client computer unique IP address, server IP address, and the nonce value. The hash value is transmitted through the client computer (12) as an authenticator for accessing the services, whereby the server (14) reproduces the authenticator by utilizing the same hash algorithm and parameters. A compare between the reproduction and the transmitted authenticator is accomplished. If they match, the grant of an access to the server (14) and services is authorized. By utilizing the client computer (12) unique IP address in the authenticator it prevents a MITM computer (16), having a different IP address, from addressing the server with a matching authenticator. The present invention also comprises an authenticator signal and a medium for carrying the signal.